EXHIBIT 1

UNITED STATES DISTRICT COURT
WESTERN DISTRICT OF NEW YORK

MOOG INC., Plaintiff, v. SKYRYSE, INC., ROBERT ALIN PILKINGTON, MISOOK KIM, and DOES NOS. 1–50. Defendants.	Civil Action No. 1:22-cv-00187

FORENSIC PROTOCOL ORDER

I. Purpose and Limitations

1. The protocol described in this Order is intended to govern material and devices made available for inspection through neutral forensic vendor iDiscovery ("iDS") in compliance with the March 11, 2022 stipulated order at Dkt. 25.

2. The protocol described in this Order shall not constitute a waiver of any kind, including a waiver of any challenge regarding the admissibility of evidence, a waiver of any applicable privilege, or a waiver of any argument regarding Moog's failure to identify its purportedly misappropriated trade secrets with the requisite degree of particularity. Any production of materials in connection with this Order shall be done pursuant to, and in accordance with, any Protective Order entered in this Action.

3. The protocol described in this Order concerns forensic discovery as to specifically identified repositories of electronically stored information and does not waive or prejudice any Party's right or entitlement to take discovery from any other repository or data source, including

based on information elicited pursuant to this Order.

4. At all times, iDS shall be guided by its professional judgement and experience, and shall work to effectuate the foregoing goals. The specific provisions set forth below are intended as exemplary guides. If iDS determines there are better, more complete, or more efficient means of effectuating the above, iDS shall propose those alternatives to the Parties. Until and unless the Parties agree to any such alternative, iDS shall continue the inspection as set forth below.

II. Forensic Imaging of Devices

1. iDS shall make forensically sound images of all physical devices made available for inspection (the "Images") using industry-standard tools and methods, and perform all analyses using those Images. The Producing Party shall provide iDS with any usernames, access passwords, decryption keys, two-factor authentication codes, or other information needed to allow iDS to perform the forensic imaging and other procedures as provided in this Order. Any original physical devices shall, at all times, be preserved unaltered.

2. For all physical devices made available for inspection, iDS shall (i) take clear photographs of devices from all angles with sufficient detail to show markings and text; and (ii) record the specifications and serial number identifiers, including internal/embedded serial numbers, for the devices to document their current state and physical properties.

3. iDS shall maintain a confidential copy of the Images until Final Resolution of this litigation (with "Final Resolution" defined as entry of a non-appealable judgment or order dismissing the case or thirty days after the time to appeal or seek relief from any judgment or order resolving the case has lapsed and no appeal is taken or relief sought).

III. Identifying Potential Moog Confidential Information

1. The data from the Images shall be subjected to a standard eDiscovery workflow whereby user data is extracted, processed, and indexed using industry-standard methods and tools such as Relativity or Nuix Discover.

2. For each Image, iDS shall create a "red flag report." To generate these reports, iDS shall exercise independent judgment to uncover forensic evidence of whether, and the extent to which, the examiner believes potential Moog confidential information—comprised of some or all of the Target Documents described below—was stored on, used by, transferred to, or transferred from, the devices provided for inspection.

3. The Parties shall jointly provide the following information regarding the "Target Documents" to iDS:

   a. The Moog Filename List, as further modified by Moog to remove all files that did not originate with or belong to Moog; and

   b. The Moog Hash Value List, as further modified by Moog to remove all files that did not originate with or belong to Moog.

4. The Target Documents comprise the universe of potential Moog confidential information for purposes of this Order. However, a Target Document is not presumptively a Moog confidential document, nor does it create a presumption of any need for further analysis. iDS shall exercise independent judgment to determine whether a Target Document is likely to comprise or contain information confidential to Moog such to trigger a flag for purposes of the "red flag" report. Moog still bears the burden to demonstrate that each of the files identified as triggering a flag in a red flag report, and any file identified as potentially containing Moog confidential information, is in fact confidential to Moog.

5. Once generated, iDS shall provide the red flag reports as well as all underlying data relied upon to generate the reports. Underlying data shall include (i) a file list of the Image's contents relied on to generate the red flag reports, including all files with all available metadata; (ii) a .LNK report with all available information regarding file access; (iii) browser history; (iv) a list of deleted files able to be recovered or identified through file carving or other techniques; (v) a report of all external device connections and evidence of file transfer to and from such external devices; (vi) a report of any forensic countermeasures that may have been taken on a device (e.g., use of file shredding, scrubbing, or similar software or programs); and/or (vii) any other raw forensic data iDS deems potentially related to the receipt, storage, use, access, transfer, and or deletion of potential Moog confidential information.

6. The reports and data shall be provided in the first instance to counsel for Defendants so that counsel for Defendants may determine whether any information should be withheld for privilege. Defendants shall have two weeks to conduct this review, and shall seek redaction of material only for reasons related to privilege. After this two-week period, the reports and data, with any privilege redactions, shall be provided to counsel for Moog. At the time such reports and data are provided to Moog, Defendants will serve privilege logs adequate to support their respective assertions of privilege.

IV. Communications with iDS

1. The Parties shall not engage in *ex parte* communications with iDS, with the exception of: (i) communications to orally configure or troubleshoot licensing issues with respect to the software tools to be used for inspection; (ii) the transmission in the first instance of the reports and underlying data to Defendants for their two-week review; or (iii) as expressly permitted elsewhere in this Order. Communications related solely to financial matters such as invoices, payment, and billing questions shall not be considered *ex parte* communications.

2. When a Producing Party provides materials to iDS for inspection, the Producing Party must simultaneously notify all other Parties regarding this provision (e.g., by copying other Parties on the communications to iDS regarding the provision of materials for inspection) and also identify the materials with sufficient particularity.

3. All written communications with the exception of communications related solely to financial matters, which need not copy any other Party, between a Party and iDS must be copied to all other Parties in the action.

DATED: April __, 2022

SHEPPARD, MULLIN, RICHTER & HAMPTON LLP HODGSON RUSS LLP By: _____ Counsel for Plaintiff Moog Inc.	GIBSON, DUNN & CRUTCHER, LLP HARRIS BEACH PLLC By: _____ Counsel for Defendant Skyryse, Inc.
LOCKE LORD LLP By: _____ Counsel for Defendant Robert Alin Pilkington	LOCKE LORD LLP By: _____ Counsel for Defendant Misook Kim

IT IS SO ORDERED.

DATED: _____, 2022	_____ The Honorable Jeremiah J. McCarthy